International Journal of Future Generation Communication and Networking
Vol. 9, No. 5 (2016), pp. 43-48
http://dx.doi.org/10.14257/ijfgcn.2016.9.5.05

False Alarm Method for Detecting Selfish Node in Manet

M. Sandhini[1] and S. Saravanan[2]

[1]*Master of Technology, Department of Computer Science and Engineering, Rajiv Gandhi College of Engineering &Technology, India*
[2]*Assistant Professor (SL.G), Department of Computer Science and Engineering, Rajiv Gandhi College of Engineering &Technology, India*
[1]*itsmesandhini18@gmail.com and* [2]*barathsamraj@yahoo.co.in*

Abstract

Several Techniques and requirements including intrusion detection system are used to detect the behavior of selfish node in MANET. The main requirement is that the system must be effective i.e. it must detect a substantial percentage of intrusions in the supervised systems, while keeping the false alarm rate at an acceptable level. The existing system in the literature uses the watchdog method to detect the selfish nodes only to certain extent in the network. In order to detect the selfish nodes in the entire network the proposed system uses a false alarm method. In the false alarm method the reason for generation of alarm is found. The degree of selfishness is calculated to confirm the behavior of the selfish node. If the value of the selfish node is more than the threshold then the alarm is due to the nodes behavior else the alarm is due to the network disconnections. The network disconnections are detected using false alarm detection algorithm. The detection of the false alarm leads to better performance in the overall network.

Keywords*: intrusion detection system, false alarm method, selfish node, nodes behavior*

1. Introduction

Mobile ad hoc network, the mobility and resource constraints of mobile nodes may lead to network partitioning or performance decay. Several data replication techniques have been proposed to minimize performance degradation. Most of them assume that all mobile nodes collaborate fully in terms of sharing their memory space. In reality, however, some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes. These selfish nodes could then reduce the overall data accessibility in the network. Mobile Ad hoc Networks don't rely on unnecessary fixed infrastructure and can be installed without base station and dedicated routers. The nodes in these networks have limited battery power and bandwidth, and each node needs the assistance of others to get its packets forwarded.

The operation of MANETs does not depend on preexisting infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network. A node may act selfishly, i.e., using its limited resource only for its own benefit, since each node in a MANET has resource limitations, such as battery and storage limitations. A node would like to enjoy the benefits provided by the resources of other nodes, but it may not make its own resource available to help others. Such selfish behavior can potentially lead to a wide range of problems for a MANET.

ISSN: 2233-7857 IJFGCN

Mobile ad hoc networks (MANETs) rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But supporting a MANET is a cost-intensive action for a mobile node. Detecting routes and forwarding packets consumes local CPU time, memory, network-bandwidth, and last but no smallest amount of energy. Therefore there is a strong motivation for a node is to reject packet that forwarding to others, while at the same time using their facilities to deliver own data.

2. Related Works

P. Michiardi and R. Molva describes "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Manet" that price-based system uses virtual cash to control the transactions of a packet forwarding service. Although these two kinds of systems have been widely used, very little research has been devoted to investigating the effectiveness of the node cooperation incentives provided by the systems. By this enhancement, they use game theory to analyze the cooperation incentives provided by these two systems and by a system with no cooperation incentive strategy. They find that the strategies of using a threshold to determine the trustworthiness of a node in the reputation system and of rewarding cooperative nodes in the price based system may be manipulated by clever or wealthy but selfish nodes. Illumined by the investigation results, they propose and study an integrated system [1].

C. K. N. Shailender Gupta and C. Singla describesimpact of selfish node concentration in Manet address the issue of reliable information distribution in highly powerful cellular ad hoc systems. Still network topology makes traditional ad hoc redirecting methods not capable of providing acceptable performance. In the face of frequent they be link crack due to node flexibility, significant information packages would either get lost, or experience long latency before recovery of connection. Motivated by opportunistic redirecting, they recommend a novel MANET redirecting method which uses the stateless property of geographical redirecting and transmitted nature of wireless method. Besides selecting the next hop, several sending applicants are also clearly specified in case of link crack. Utilizing on such natural back-up in the air, damaged route can be retrieved in regular basis. The potency of the participation of sending applicants against node flexibility, as well as the expense due to opportunistic sending is examined.

Through simulator, they further validate the performance and performance of POR: high bundle distribution rate is obtained while the delay and duplication are the smallest. On the other hand, got from geographical redirecting, the issue of interaction gap is also examined. To work with the multicast sending style, a exclusive destination-based gap managing plan is suggested. By momentarily modifying the direction of information flow, the benefits of selfish sending as well as the sturdiness brought about by opportunistic redirecting can still be obtained when managing interaction voids. Traditional gap managing method works badly in cellular surroundings while VDVH works quite well [2].

S.abbas, m.merabti, Lightweight sybil attack detection in manets address Confidentiality ensure that the information is inaccessible to unauthorized users. In WSNs, data in the sensors should be encrypted in a way that it can only be read by the sink. In some scenarios, data from the nodes will not be sent to the sink in a single hop.

Sink visits a point for data collection which can be few hops away from the node and the data has to be sent through other nodes. In these cases the intermediate nodes should not be able to read the transmitted information. Data confidentiality also prevents the read only adversary from reading the stored data in the compromised node's memory. Data integrity protects against unauthorized alteration of the data. Data integrity can be achieved only if the network has the ability to detect the manipulations done to the data by unauthorized parties, *i.e.*, insertion, substitution and deletion. An encryption based symmetric cryptography is used to detect the misbehaving node in the sensor network [3].

L. Buttyan and J.P. Hubaux, "stimulating cooperation in self organizing Mobile ad hoc networks address tasks are conducted based on the cooperation of nodes in the networks. However, since the nodes are usually constrained by limited computation resources, selfish nodes may refuse to be cooperative. Reputation systems and price-based systems are two main solutions to the node noncooperation problem.

A reputation system evaluates node behaviors by reputation values and uses a reputation threshold to distinguish trustworthy nodes and untrustworthy nodes. A price-based system uses virtual cash to control the transactions of a packet forwarding service. Although these two kinds of systems have been widely used, very little research has been devoted to investigating the effectiveness of the node cooperation incentives provided by the systems. In this paper, we use game theory to analyze the cooperation incentives provided by these two systems and by a system with no cooperation incentive strategy. We find that the strategies of using a threshold to determine the trustworthiness of a node in the reputation system and of rewarding cooperative nodes in the price-based system may be manipulated by clever or wealthy but selfish nodes. Illumined by the investigation results, we propose and study an integrated system. Theoretical and simulation results show the superiority of the integrated system over an individual reputation system and a price-based system in terms of the effectiveness of cooperation incentives and selfish node detection [4].

J. Hortelano, j. C. Ruiz, and p. Manzoni, "evaluating the usefulness of watchdogs for intrusion detection in vanets addressVanet's are easy to release and can considerably effect the efficiency of systems. Although the identification of a node can be confirmed through cryptographic verification, traditional protection techniques are not always suitable because of their expense specifications. In this document, we recommend to use spatial information, actual residence associated with each node, hard to falsify, and not a few cryptography, as the foundation for 1) discovering spoofing attacks; 2) identifying the variety of assailants when several opponents disguised as the same node identity; and 3) localizing several opponents. We recommend to use the spatial connection of obtained indication durability (RSS) got from wifi nodes to identify the spoofing strikes. We then come up with the issue of identifying the variety of assailants as a multiclass recognition issue.

Cluster-based systems are designed to figure out the variety of assailants. When the training information are available, we discover using the Assistance Vector Devices (SVM) method to further enhance the precision of identifying the variety of assailants. Moreover, we designed a recognition and localization system that can localize the roles of several assailants [5].

Enrique Hernandez Orallo and Manuel David Serrat Olmos describes CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes address Watchdogs are used to detect selfish nodes in computer networks. A way to reduce the detection time and to improve the accuracy of watchdogs is the collaborative approach. A collaborative watchdog based on contact dissemination of the detected selfish nodes. Then, they introduce an analytical model to evaluate the detection time and the cost of this collaborative approach. A way to reduce the detection time of selfish (or non-cooperative) nodes in a network is the collaborative watchdog. This paper introduces an efficient approach to reduce the detection time of selfish nodes based on contact dissemination. If one node has previously detected a selfish node using its watchdog it can spread this information to other nodes when a contact occurs. They say that a node has a positive if it knows the selfish node. The detection of contacts between nodes is straightforward using the node as watchdog [6].

3. System Analysis

In the system we have implemented a selfish node detection method and novel replica allocation techniques to handle the selfish replica allocation. The proposed schemes are inspired by the real world observations in economics in terms of credit risk and in human friendship management in terms of choosing one's friends completely at one's own decision. We have applied the concept of credit risk from economics to detect selfish nodes. Each and Every node in a specific network calculates credit risk information on other connected nodes individually to measure the degree of selfishness. The system performances are extensively significant in the detection of attacker and to provide congestion control at MANET.

Extensive simulation shows that the proposed strategies outperform the cooperative replica allocation techniques in terms of data accessibility, communication cost, and query delay. The False alarm at selfishness will decrease the data flow of the network. By using our technique we will pass the information as it is not by selfishness. So no significant change will occur except choosing for alternative routes. As a part future, we plan to consider all the replication strategies and network disconnections suited for various consistency levels and with increase in security against various attacks. Our next goal will be to conduct an analytical study of the impact of node mobility on network performance with misbehaving nodes. We plan then to design and evaluate a collaborative security scheme that solves the selfishness problem, analyzing the effects of such mechanism on network throughput and communication delay.

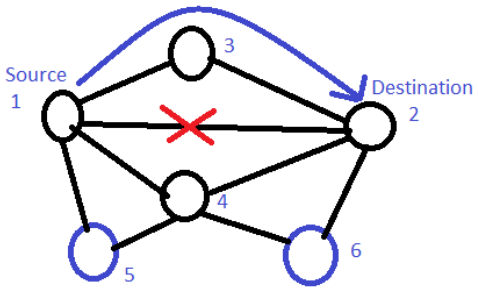

Figure 1.1. Data Transfer between Node 1 and Node 2

The Figure shows the data transfer between source and destination and the blue rings are selfish node and Red Cross are path disconnected between node 1 and 2.

3.1. Advantages

- Error detection and correction is very low and their resistance to fault attacks.
- OpenFlow protocol may eventually become one of the most effective technologies for the development of various innovations in the field of network security.
- Easily to find the fault attackers and bug is free to verify it.

4. Conclusion

MANET as a technology can only become successful and popular if the challenges related to routing and intrusion detection, as described in this report, are adequately addressed The proposed combined algorithm (Node Replacement and False alarm) with the decision making based on fuzzy rules has shown more accurate results than the algorithms used alone. By detecting attacks approximately corresponds to the results is obtained to that of the number of lines of code decreased and as well as the opportunity to easily integrate various external libraries and modules, thus greatly simplifies the

implementation of the algorithms and decision-making system. The opportunity provides a unique for effective detection and containment of network security problems, allowing the integration of complex network security applications in large networks.

References

[1] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism To Enforce Node Cooperation In Mobile Ad Hoc Networks".
[2] C. K. N. S. Gupta and C. Singla, "Impact Of Selfish Node Concentration In Manets", International Journal on Wireless Mobile Networks, vol. 3, no. 2, **(2011)**, pp. 29–37.
[3] S. Abbas, M. Merabti, D. L. Jones and K. Kifayat, "Lightweight Sybil Attack Detection in Manets", IEEE system Journal, vol. 7, no. 2, **(2013)**, pp. 236–248.
[4] L. Buttyan and J. P. Hubaux "stimulating cooperation in self organizing Mobile ad hoc networks", mobile netw. Appl., vol. 8, **(2003)**, pp. 579–592.
[5] J. Hortelano, J. C. Ruiz and P. Manzoni, "evaluating the usefulness of watchdogs for intrusion detection in vanets", Proceedings on .int. Conf. Commun. Workshop, **(2010)**, pp. 1–5.
[6] E. H. Orallo, M. D. S.t Olmos, J. C. Cano, C. T. Calafate and Pietro Manzoni, "COCOWA: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes", IEEE TRANSACTIONS ON MOBILE COMPUTING, vol. 14, no. 6, **(2015)**.
[7] C. Toh, D. Kim, S. Oh, and H. Yoo, "The controversy of selfish nodes in ad hoc networks", Proceedings on. Adv. Commun. Technology, vol. 2, **(2010)**, pp. 1087–1092.
[8] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in DSR based ad-hoc networks", Proceedings on IEEE Global Telecommunication. Conf., **(2002)**, pp. 178–182.
[9] Y. Zhang, W. Lee and Y. A. Huang, "Intrusion detection techniques for mobile wireless networks", Wireless Netw., vol. 9, no. 5, **(2003)**, pp. 545–556.
[10] S. Zhong, J. Chen and Y. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks", Proceedings on IEEE Conf. Comput. Communication, vol. 3, **(2003)**, pp. 1987–1997.

Authors

M. Sandhini, she is pursuing M.Tech. Pursued B.Tech (Information Technology) from Pondicherry University in 2014. Her areas of interest includes networking, Adhoc sensor networks.

S. Saravanan, he is an Asst. Professor (Selection Grade), Computer Science department. Rajiv Gandhi college of Engineering and technology, Pondicherry, India. Qualification: B.E (Elecronics Communication) M.S (Information Technology) M.E (Computer science) M.Tech (Communication system) MBA (Education Management) Pursuing Ph.D. (BME).